UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/594,719	06/16/2000	Scott Moskowitz	066112.0137	2341

7590 10/18/2005

Scott A. Moskowitz
BLUE SPIKE, INC.
16711 Collins Avenue, #2505
Miami, FL 33160

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 10/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/594,719	MOSKOWITZ ET AL.	
	Examiner	Art Unit	
	Brandon S. Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 July 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-76* is/are pending in the application.

4a) Of the above claim(s) *73-76* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-72* is/are rejected.

7)☒ Claim(s) *17 and 47* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 August 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *8-24-00 & 7-10-02*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Restriction Requirement

1. Applicant's traversal to the restriction requirement has been considered, but is not persuasive in view of the following reasons: 35 U.S.C. 101 states that "whoever invents... may obtain **a** patent." The emphasis is placed on 'a' meaning one. If the instant application were to go to allowance, the applicant would obtain multiple patents from one application. Accordingly, the restriction requirement was/is proper.

Specification

2. The disclosure is objected to because of the following informalities:

- The "CROSS-REFERENCE TO RELATED APPLICATIONS" section needs updated to reflect applications that have matured into patents. This is found on page 1 of the specification. Appropriate correction is required.

Claim Objections

3. Claims 17 and 47 objected to because of the following informalities: claim 17 should say "identification" instead of "indemnification" and claim 47 should be dependent upon 45, not 42. Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Senoh (U.S. Patent No. 6,240,121) in view of Kato et al. (U.S. Patent No. 6,301,663).

Regarding claims 1, 2, 10, 37, and 45, Senoh teaches a method/system of securing a data signal comprising the steps of:

- Applying a data reduction technique to reduce the data signal into a reduced data signal (fig. 1, ref. num 11);
- Subtracting said reduced data signal from the data signal to produce a remainder signal (fig. 1, ref. num 24);
- Embedding a first watermark into said reduced data signal to produce a watermarked, reduced data signal (fig. 1, ref. num 23); and
- Adding said watermarked, reduced data signal to said watermarked remainder signal to produce an output signal (fig. 1, ref. num 31).

Senoh does not teach embedding a second watermark into said remainder signal to produce a watermarked remainder signal.

Kato et al. teaches embedding a second watermark into said remainder signal to produce a watermarked remainder signal (col. 9, lines 43-52).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine embedding a second watermark into said remainder signal, as taught by Kato et al., with the method/system of Senoh. It would have been obvious for such modifications because embedding a watermark signal into each of the reduced signals prevents deliberate or accidental attempts at removing the watermarked data completely, and therefore the watermark will remain detectable despite tampering attempts (see col. 7, lines 50-61 of Senoh).

Regarding claims 3, 15, 28, and 47, Senoh as modified by Kato et al. teaches wherein at least one of the watermarks is embedded using at least one cryptographic key (see col. 9, lines 47-52 of Kato et al.).

Regarding claims 4, 16, and 29, Senoh as modified by Kato et al. teaches wherein at least one of the watermarks is embedded using a cryptographic key pair (see col. 8, lines 7-14 of Kato et al.).

Regarding claims 5 and 18, Senoh as modified by Kato et al. teaches wherein one key of the cryptographic key pair is publicly available while the other key of the cryptographic key pair is secret (see col. 6, lines 4-8 and lines 15-18 of Kato et al.).

Regarding claims 6, 12, 22, 34, 42, and 49, Senoh as modified by Kato et al. teaches wherein the data reduction technique comprises a data compression technique (see col. 5, lines 41-57 of Senoh).

Regarding claims 7, 13, 23, 35, and 43, Senoh as modified by Kato et al. teaches wherein the data compression technique comprises a standard lossy protocol for digital signal transmission (see col. 10, lines 58-65 of Senoh).

Regarding claims 8, 14, 24, 36, 44, and 50, Senoh as modified by Kato et al. teaches wherein the data compression technique comprises selective sampling of the data signal in a domain selected from the group comprising the time domain, bit depth domain, and the frequency domain (see col. 5, lines 41-57 of Senoh).

Regarding claims 9 and 61, Senoh as modified by Kato et al. teaches wherein at least one of said first and second watermarks is selected from the group comprising forensic watermarks and universal copy control watermarks (see col. 1, lines 24-26 of Senoh).

Regarding claims 11 and 46, Senoh as modified by Kato et al. teaches wherein the step of subtracting is comprised of

- Storing a copy of the data signal (see col. 9, lines 50-52 of Kato et al.); and

- Subtracting said reduced data signal from the copy of the data signal to produce a remainder signal (see fig. 1, ref. num 24 of Senoh).

Regarding claims 17 and 30, Senoh as modified by Kato et al. teaches wherein a copy of said keys is maintained at a central certification authority for reference identification purposes (see col. 6, lines 4-8 of Kato et al.).

Regarding claim 19, Senoh as modified by Kato et al. teaches further comprising repeating for a finite number of times the steps of data reduction, subtraction, and embedding (see fig. 1, ref. num 11, 24, 23, and 31 of Senoh, a finite number of times could be 1, which would be the initial time of reduction, subtraction, and embedding).

Regarding claims 20 and 25, Senoh teaches a method of securing a data signal comprising:

- Applying a data reduction technique to reduce the data signal into a reduced data signal (fig. 1, ref. num 11);
- Subtracting said reduced data signal from the data signal to produce a remainder signal (fig. 1, ref. num 24); and
- Adding said encrypted, reduced data signal to said encrypted remainder signal to produce an output signal (fig. 1, ref. num 31).

Senoh does not teach using a first cryptographic technique to encrypt the reduced data signal to produce an encrypted, reduced data signal; or using a second cryptographic technique to encrypt the remainder signal to produce an encrypted remainder signal.

Kato et al. teaches using a first cryptographic technique to encrypt the reduced data signal to produce an encrypted, reduced data signal (fig. 1, ref. num 4); and using a second cryptographic technique to encrypt the remainder signal to produce an encrypted remainder signal (fig. 1, ref. num 9).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine using a first and second scrambling technique, as taught by Kato et al., with the method/system of Senoh. It would have been obvious for such modifications because scrambling/encrypting each of the reduced signals prevents deliberate or accidental attempts at removing the scrambled/encrypted data completely, and therefore the scrambling/encryption will remain intact despite tampering attempts (see col. 7, lines 50-61 of Senoh).

Regarding claims 21, 26, 33, and 38, Senoh as modified by Kato et al. teaches wherein said first and second scrambling techniques are identical (see col. 5, lines 48-50 of Kato et al.).

Regarding claims 27 and 39, Senoh as modified by Kato et al. teaches wherein at least one of said first and second cryptographic techniques is a watermarking technique for embedding at least one digital watermark in a signal (see fig. 1, ref. num 23 of Senoh).

Regarding claims 31 and 40, Senoh as modified by Kato et al. teaches wherein at least one of said first and second cryptographic techniques is a scrambling technique (see col. 15, lines 31-44 of Kato et al.).

Regarding claims 32 and 41, Senoh as modified by Kato et al. teaches wherein one of said first and second cryptographic techniques is a watermarking technique for embedding a digital watermark in a signal and the other is a scrambling technique (see col. 6, line 26-29 of Senoh and col. 15, lines 31-44 of Kato et al.).

Regarding claim 48, Senoh as modified by Kato et al. teaches wherein said at least one digital watermarking algorithms comprises two different digital watermarking algorithms (see fig. 4, ref. num 22 and 25 of Kato et al.).

Regarding claim 51, Senoh teaches a method for securing a data signal comprising the steps of:

- Evaluating the data signal to determine its characteristics and reducibility (col. 5, lines 41-57);

- Selecting at least one appropriate data reduction technique for the data signal based on the data signal's characteristics (col. 5, lines 41-57);
- Applying said at least one appropriate data reduction technique to the data signal to produce a reduced data signal (fig. 1, ref. num 11);
- Embedding at least one digital watermark in the reduced data signal (fig. 1, ref. num 23); and
- Supplying an output signal corresponding to the data signal, said output signal comprising said watermark and said reduced data signal (fig. 1, ref. num 31).

Senoh does not specifically teach supplying an output signal.

Kato et al. teaches an output signal is supplied to the optical medium (fig. 4, ref. num 27).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine supplying the output signal, as taught by Kato et al., with the method/system of Senoh. It would have been obvious for such modifications because supplying an output signal comprising copy protected data entitles the proper user to use the data without the worries of a third party stealing the data.

Regarding claim 52, Senoh as modified by Kato et al. teaches wherein the evaluation step comprises:

- Dividing the data signal into a plurality of discrete data substreams (see col. 5, lines 41-57 of Senoh); and
- Evaluating each of said plurality of discrete data substreams to determine its characteristics and reducibility (see col. 5, lines 41-57 of Senoh); and wherein the selecting step comprises:
- Selecting at least one appropriate data reduction technique for each of said plurality of discrete data substreams based on the substreams characteristics (see col. 5, lines 41-57 of Senoh).

Regarding claim 53, Senoh as modified by Kato et al. teaches wherein the appropriateness of said at least one data reduction technique is determined with reference to data signal characteristics selected from at least one of: a desired output quality for an output signal; a desired data reduction ratio; audio character of data; video character of data; text character of data; executable software character of data (see col. 5, lines 41-57 of Senoh).

Regarding claim 54, Senoh as modified by Kato et al. teaches wherein the same data reduction technique is used for each of said plurality of data substreams (see col. 5, lines 41-57 and fig. 2 of Senoh).

Regarding claim 55, Senoh as modified by Kato et al. teaches further comprising the steps of performing one of the following techniques upon at least one of said

plurality of data substreams: a scrambling technique; an encryption technique (see fig. 4, ref. num 25 of Kato et al.).

Regarding claim 56, Senoh as modified by Kato et al. teaches wherein at least one of said steps of watermarking, scrambling, or encrypting comprises applying at least one cryptographic key (see fig. 4, ref. num 25 of Kato et al.).

Regarding claim 57, Senoh as modified by Kato et al. teaches further comprising deriving said at least one cryptographic key at least in part from the data signal (see fig. 1, ref. num 6 of Kato et al.).

Regarding claim 58, Senoh as modified by Kato et al. teaches further comprising deriving said at least one cryptographic key independently of the data signal (see fig. 1, ref. num 6 of Kato et al.).

Regarding claim 59, Senoh as modified by Kato et al. teaches wherein said step of evaluating the data signal comprises analyzing the data signal with a computer processor implementing an algorithm for analysis of signal characteristics (see fig. 1, ref. num 11 and fig. 2 and col. 5, line 41 through col. 6, line 26 of Senoh).

Regarding claim 60, Senoh teaches a method for the protection of a data signal, comprising the steps of:

- Defining and analyzing a plurality of data substreams within the data signal (col. 5, lines 41-57).

Senoh does not teach associating at least one key or key pair with data reduction digital watermarking for at least one of said data substreams.

Kato et al. teaches associating at least one key or key pair with data reduction digital watermarking for at least one of said data substreams (fig. 1, ref. num 6).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine associating a key with data reduction for at least one substream, as taught by Kato et al., with the method/system of Senoh. It would have been obvious for such modifications because the associated key can be recovered to restore the data substream to its original data (see col. 8, lines 7-35 of Kato et al.).

The combination of Senoh and Kato et al. now teach employing said at least one key or key pairs for at least one step selected from the group of: identifying at least one associated watermark; encoding at least one associated watermark; detecting at least one associated watermark; or decoding at least one associated watermark (see fig. 3 of Kato et al.).

Claims 62-72 are rejected under 35 U.S.C. 103(a) as being unpatentable over Senoh (USPN '121).

Regarding claim 62, Senoh teaches a method for protected distribution of a data file comprising:

- Embedding one or more digital watermarks in the data file using data reduction techniques in creating said digital watermark (fig. 1, ref. num 11 and 23).

Senoh does not specifically teach distributing the digitally watermarked file to an end user. However, Senoh discloses preventing unauthorized copying by third parties – which implies the watermarked file will be transmitted to someone (fig. 1, ref. num 31).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to distribute the watermarked file to an end user. It would have been obvious for such modifications because transmission of copy protected data entitles the proper user to use the data without the worries of a third party stealing the data.

Regarding claim 63, Senoh teaches wherein the use of data reduction techniques comprises creation of a reduced portion of the data file and a remainder portion of the data file (col. 5, lines 41-57).

Regarding claim 64, Senoh teaches wherein the embedding step comprises embedding one or more digital watermarks in each of the reduced portion and the remainder portion of the data file (col. 6, lines 27-45).

Regarding claim 65, Senoh teaches further comprising combining said watermarked, reduced portion with said watermarked, remainder portion to produce the digitally watermarked file (col. 6, lines 45-52).

Regarding claim 66, Senoh teaches wherein said step of embedding said one or more digital watermarks in the data file is performed on a central computer server and wherein said distributing step is performed by transmitting the digitally watermarked file from the central computer server to an end user output device (col. 1, lines 15-26).

Regarding claim 67, Senoh teaches wherein said step of distributing comprises transmitting the digitally watermarked file over a public data network (col. 1, lines 15-26).

Regarding claim 68, Senoh teaches wherein said step of distributing comprises transmitting the digitally watermarked file over the Internet (col. 1, lines 15-26).

Regarding claim 69, Senoh teaches further comprising the step of supplying the end user with means for detecting information about said digital watermark (fig. 5 and col. 9, lines 17-56).

Regarding claim 70, Senoh teaches wherein said data file comprises a file selected from the group containing music files, audio files, video files, still image files, streaming media files, and executable computer software files (col. 1, lines 15-26).

Regarding claim 71, Senoh teaches wherein at least one of said digital watermarks created using data reduction comprises a universal copy control watermark for prevention of unauthorized data file copying (col. 1, lines 24-26).

Regarding claim 72, Senoh teaches wherein at least one of said digital watermarks created using data reduction comprises a forensic watermark for tracing at least a portion of the distribution history of the data file (col. 1, lines 24-26).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brenda Hoff

BH

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100